PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Eduard ERHARDT

Docket No: Q76086

Appln. No.: 10/600,643

Group Art Unit: 2151

Confirmation No.: 6122

Examiner: Not Yet Assigned

Filed: June 23, 2003

For: COMPUTER SYSTEM CONNECTED TO A DATA COMMUNICATIONS NETWORK

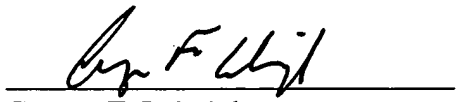
SUBMISSION OF PRIORITY DOCUMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Submitted herewith is a certified copy of the priority document on which a claim to priority was made under 35 U.S.C. § 119. The Examiner is respectfully requested to acknowledge receipt of said priority document.

Respectfully submitted,



George F. Lehnigk
Registration No. 36,359

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE
23373
CUSTOMER NUMBER

Enclosures: Germany 100 64 658.1
GFL/plr
Date: October 31, 2003

BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen:	100 64 658.1
Anmeldetag:	22. Dezember 2000
Anmelder/Inhaber:	Siemens Aktiengesellschaft, München/DE
Bezeichnung:	Rechneranordnung, die an ein Datenübertragungsnetz anschließbar ist
IPC:	G 06 F 17/60

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 10. Juli 2003
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Agurks

A 9161
06/00
EDV-L

Beschreibung

Rechneranordnung, die an ein Datenübertragungsnetz anschließbar ist

Die Erfindung betrifft eine Rechneranordnung, die an ein Datenübertragungsnetz, z. B. Internet oder Intranet, angeschlossen ist. Solche Rechneranordnungen, meist einzelne Rechner, wie z. B. PCs, sind in zunehmendem Maße Computerviren und unerlaubten Zugriffen auf interne Daten ausgesetzt. Virenscanner können in der Regel nur bekannte Computerviren erkennen und beseitigen, nicht aber solche Viren, die völlig neu sind und gänzlich andere Strukturen als bisher bekannte Viren aufweisen. Insbesondere bei Rechnern in Verwaltungen, Banken, Versicherungen, der Industrie, z. B. Bedienen und Beobachten von Automatisierungssystemen, die zunehmend über öffentliche Datenübertragungsnetze mit anderen Rechneranordnungen, z. B. zentralen Leitstellen, kommunizieren, kann die Infizierung mit Computerviren zu immensen Schäden führen. So können als Trojaner bezeichnete Programme in den Rechner eingeschleust werden, die, z. B. als Nutzprogramm getarnt, im Verborgenen interne Daten ausspähen und diese an eine externe Stelle übermitteln.

Der Erfindung liegt daher die Aufgabe zugrunde, einen sicheren Schutz gegen Computerviren, unerlaubte Zugriffe auf interne Daten und Datenverlust im Falle einer Infizierung zu erreichen.

Gemäß der Erfindung wird die Aufgabe dadurch gelöst, dass eine Rechneranordnung, die an ein Datenübertragungsnetz anschließbar ist, einen ersten Rechner und einen davon unabhängigen redundanten, zweiten Rechner aufweist, wobei sich beide Rechner durch Vergleich ihrer Arbeitsergebnisse abgleichen, wobei der Empfang von Daten aus dem Datenübertragungsnetz auf den ersten Rechner und das Senden von Daten auf das Datenübertragungsnetz auf den zweiten Rechner beschränkt ist,

wobei zumindest die Erst-Verarbeitung von empfangenen Daten auf den ersten Rechner beschränkt ist und wobei von dem ersten Rechner empfangene, nicht überprüfte oder nicht überprüfbare Daten nur verschlossen, d. h. nicht verarbeitbar, auf dem zweiten Rechner gespeichert werden.

Die erfindungsgemäße Rechneranordnung besteht also aus zwei parallelen Rechnern, die praktisch den gleichen Hardwareaufbau aufweisen und mit gleicher Software konfiguriert sind. Beide Rechner arbeiten parallel, abwechselnd oder arbeitsteilig, wobei sie sich jedoch regelmäßig durch Vergleich ihrer Arbeitsergebnisse, beispielsweise durch Quersummenüberprüfung oder Vergleich vorgegebener Daten, abgleichen. Der Abgleich kann z. B. durch den Anwender ausgelöst oder automatisch beispielsweise bei Programmende, beim Schließen von Dateien, bei der Ein- und Ausgabe von Daten oder bei Speicherzugriffen gestartet werden. Zwischen den beiden Rechnern werden Daten nur dann ausgetauscht bzw. angebotene Daten nur dann übernommen, wenn die von den Rechnern gelieferten Arbeitsergebnisse gleich sind. Im Rahmen des Abgleichs können daher aufgrund von unterschiedlichen Arbeitsergebnissen der beiden Rechner Fehlfunktionen bzw. verfälschte Daten erkannt werden.

Um die geforderte Sicherheit zu erreichen, sind der Empfang von Daten aus dem Datenübertragungsnetz und zumindest die Erst-Verarbeitung der empfangenen Daten auf den ersten Rechner und das Senden von Daten auf das Datenübertragungsnetz auf den zweiten Rechner beschränkt. Dies kann durch eine entsprechende hardware- oder softwaremäßige Sende-Sperre bzw. Empfangs-Sperre erfolgen. Anstelle der Sende-Sperre kann beispielsweise auch vorgesehen werden, dass in dem ersten Rechner nur empfangene Daten speicherbar sind, so dass ein Senden von anderen als den empfangenen Daten nicht möglich ist. Im Rahmen der auf den ersten Rechner beschränkten Erst-Verarbeitung der empfangenen Daten können diese überprüft werden, wobei nur überprüfte Daten von dem zweiten Rechner

unverschlossen, d. h. verarbeitbar, übernommen und abgespeichert werden können. Bei E-mails überprüfbare Daten sind beispielsweise die Adresse des Senders, der Betrefftext sowie weitere Teildaten, die je nach Softwareprodukt vollständig überprüfbar sind, so z. B. Textformate, nicht jedoch Makros. Die Überprüfung der Daten erfolgt dabei vorzugsweise unabhängig auf beiden Rechnern, wobei es nur nach einem Ergebnisabgleich zu einer Abspeicherung der Daten auf dem zweiten Rechner kommt. Von dem ersten Rechner empfangene, nicht überprüfte oder nicht überprüfbare Daten werden nur verschlossen (gekapselt), d. h. nicht verarbeitbar, von dem zweiten Rechner entgegengenommen. Dies gilt gleichermaßen für durch Verarbeitung dieser Daten auf dem ersten Rechner erzeugte neue Daten. Solche verschlossenen Daten können auf dem zweiten Rechner weder geöffnet noch verarbeitet werden, sondern nur als Anhang beispielsweise an ein Sende-E-mail angefügt werden.

Auf diese Weise wird erreicht, dass der zweite, redundante Rechner, der aufgrund von Hardware- oder Softwaremaßnahmen empfangsuntüchtig ist, frei von Computerviren bleibt und dass auch keine Computerviren beim Senden von Daten nach außen weitergegeben werden können. Auch können keine Daten durch so genannte Trojaner abgeholt oder verfälscht werden. Wird der erste Rechner aufgrund von empfangenen Daten mit Computerviren infiziert, so wird dies bei dem Abgleichen der beiden Rechner erkannt. In diesem Fall kann durch Kopieren des Zustandes des zweiten Rechners auf den ersten Rechner dieser wieder in einen virenfreien Zustand versetzt werden, ohne dass Daten oder bereits ausgeführte Arbeiten verloren gehen.

Um auszuschließen, dass in einem zentralen Datenspeicher enthaltene interne Daten der Rechneranordnung aufgrund einer Infizierung des empfangsfähigen ersten Rechners verfälscht oder gelöscht werden, ist der unmittelbare Zugriff auf diese Daten auf den zweiten Rechner beschränkt, wobei der erste

Rechner diese Daten nur auf Anforderung über den zweiten Rechner erhält.

Bei vergleichsweise großen zu erbringenden Rechenleistungen kann ein unabhängiger redundanter, dritter Rechner vorgesehen sein, wobei sich der zweite und der dritte Rechner durch Vergleich ihrer Arbeitsergebnisse abgleichen. Im Falle eines Automatisierungssystems übernimmt z. B. der dritte Rechner Automatisierungsfunktionen, während der erste und der zweite Rechner für die Kommunikation über das Datenübertragungsnetz zuständig sind.

Im Weiteren wird die erfindungsgemäße Rechneranordnung anhand eines in der Figur der Zeichnung dargestellten Ausführungsbeispiels erläutert.

Die hier als Funktions-Blockschaltbild dargestellte Rechneranordnung besteht aus einem ersten Rechner 1, einem zweiten, redundanten Rechner 2 und einem optionalen, dritten Rechner 3. Die Rechner 1, 2 und 3 weisen, von den unten angegebenen Ausnahmen abgesehen, jeweils den gleichen Hardwareaufbau auf und sind mit der gleichen Software konfiguriert. Der Rechner 1 ist über einen Empfangstreiber 4 an einem Datenübertragungsnetz 5 angeschlossen und im Übrigen sendeuntüchtig. Der redundante Rechner 2 ist über einen Sendetreiber 6 an dem Datenübertragungsnetz 5 angeschlossen und im Übrigen empfangsuntüchtig. Der optionale, dritte Rechner 3 ist für den Fall vorgesehen, dass höhere Rechenleistungen erbracht werden sollen, wie z. B. das Bedienen und Beobachten von Automatisierungssystemen. Mit Ausnahme der Erst-Verarbeitung von empfangenen Daten, die auf den ersten Rechner 1 beschränkt ist, und der von dem dritten Rechner 3 zu erbringenden höheren Rechenleistungen werden in allen Rechnern 1, 2 und 3 die gleichen Funktionen ausgeführt, weswegen Anwender-Eingaben, die beispielsweise an einer Tastatur 7 oder einer Computermaus 8 vorgenommen werden, allen Rechnern 1, 2 und 3 parallel zugeführt werden.

In einem ersten Speicher bzw. Speicherbereich 9 werden die Arbeitsergebnisse der beiden Rechner 1 und 2 beispielsweise durch Quersummenüberprüfung usw. abgeglichen. Weitere Speicher bzw. Speicherbereiche 10 und 11 dienen zum Datenaustausch im Rahmen des Ergebnisabgleichs der beiden Rechner 1 und 2, wobei Daten nur dann ausgetauscht bzw. angebotene Daten nur dann akzeptiert werden, wenn die Arbeitsergebnisse der beiden Rechner 1 und 2 gleich sind.

Von dem Rechner 1 aus dem Datenübertragungsnetz 5 empfangene Daten, z. B. E-mails, werden im Rahmen des Datenaustauschs nur selektiv (z. B. Adresse des Senders, Betrefftext) bzw. in dem Umfang an den zweiten Rechner 2 weitergegeben, wie diese Daten vollständig überprüfbar sind (z. B. Textformate, nicht jedoch Makros). Die Prüfung wird auf beiden Rechnern 1 und 2 unabhängig ausgeführt, wobei die endgültige Übertragung und Abspeicherung in den jeweils anderen Rechner erst bei übereinstimmenden positiven Prüfergebnissen erfolgt. Im Übrigen ist die Erst-Verarbeitung von empfangenen Daten allein auf den ersten Rechner 1 beschränkt. Nicht überprüfbare empfangene Daten sowie durch Verarbeitung dieser Daten in dem Rechner 1 neu erzeugte Daten werden im Rahmen des Datenaustauschs nur in verschlossenem Zustand an den zweiten, redundanten Rechner 2 übergeben, der die verschlossenen Daten weder öffnen noch verarbeiten kann. Diese Daten können dann im verschlossenen Zustand nur als Anhang an andere zu sendende Daten, z. B. ein Sende-E-mail, angefügt werden.

Wird der erste Rechner 1 aufgrund von empfangenen Daten mit Computerviren infiziert, so wird dies bei dem regelmäßigen Abgleichen der beiden Rechner 1 und 2 erkannt. Aufgrund der oben erläuterten Sicherheitsmechanismen bei dem Datenaustausch zwischen den beiden Rechnern 1 und 2 ist ein Übergreifen der Computerviren von dem ersten Rechner 1 auf den zweiten Rechner 2 ausgeschlossen. Durch Kopieren des Zustandes des zweiten Rechners 2 auf den ersten Rechner 1 kann dieser wieder in einen virenfreien Zustand versetzt werden,

ohne dass Daten verloren gehen. Durch die oben erläuterten Sicherheitsmechanismen wird weiterhin ein unerlaubter Zugriff über das Datenübertragungsnetz 5 auf interne Daten der Rechneranordnung ausgeschlossen.

Wie bereits erwähnt, werden größere Rechenleistungen im Wesentlichen von dem optional vorgesehenen, dritten Rechner 3 erbracht, wobei der erste Rechner 1 und der zweite Rechner 2 für die Kommunikation über das Datenübertragungsnetz 5 zuständig sind. Der dritte Rechner 3 gleicht sich dabei über Speicher bzw. Speicherbereiche 12, 13 und 14 mit dem zweiten Rechner 2 ab. Aus Sicherheitsgründen hat der erste Rechner 1 keinen Zugriff auf einen zentralen Datenspeicher 15 mit gemeinsamen Daten, die nur von dem Rechner 3 und gegebenenfalls dem Rechner 2 gelesen werden können und erforderlichenfalls dem ersten Rechner 1 bereitgestellt werden.

Patentansprüche

1. Rechneranordnung, die an einem Datenübertragungsnetz (5) anschließbar ist, mit einem ersten Rechner (1) und einem davon unabhängigen redundanten, zweiten Rechner (2), wobei sich beide Rechner (1 und 2) durch Vergleich ihrer Arbeitsergebnisse abgleichen, wobei der Empfang von Daten aus dem Datenübertragungsnetz (5) auf den ersten Rechner (1) und das Senden von Daten auf das Datenübertragungsnetz (5) auf den zweiten Rechner (2) beschränkt ist, wobei zumindest die Erst-Verarbeitung der empfangenen Daten auf den ersten Rechner (1) beschränkt ist und wobei von dem ersten Rechner (1) empfangene, nicht überprüfte oder nicht überprüfbare Daten nur verschlossen, d. h. nicht verarbeitbar, auf dem zweiten Rechner (2) gespeichert werden.

2. Rechneranordnung nach Anspruch 1, dadurch gekennzeichnet, dass die empfangenen Daten in dem ersten Rechner (1) überprüft und nur überprüfte Daten dem zweiten Rechner (2) unverschlossen, d. h. verarbeitbar, zugeführt werden.

3. Rechneranordnung nach Anspruch 1, dadurch gekennzeichnet, dass die empfangenen Daten in dem ersten Rechner (1) und dem zweiten Rechner (2) unabhängig überprüft werden und dass nur übereinstimmend überprüfte Daten auf dem zweiten Rechner (2) unverschlossen, d. h. verarbeitbar, gespeichert werden.

4. Rechneranordnung nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass ein unmittelbarer Zugriff auf in einem zentralen Datenspeicher (15) enthaltene interne Daten der Rechneranordnung auf den zweiten Rechner (2) beschränkt ist und dass der erste Rechner (1) diese Daten nur auf Anforderung über den zweiten Rechner (2) erhält.

5. Rechneranordnung nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass ein unabhängiger redun-

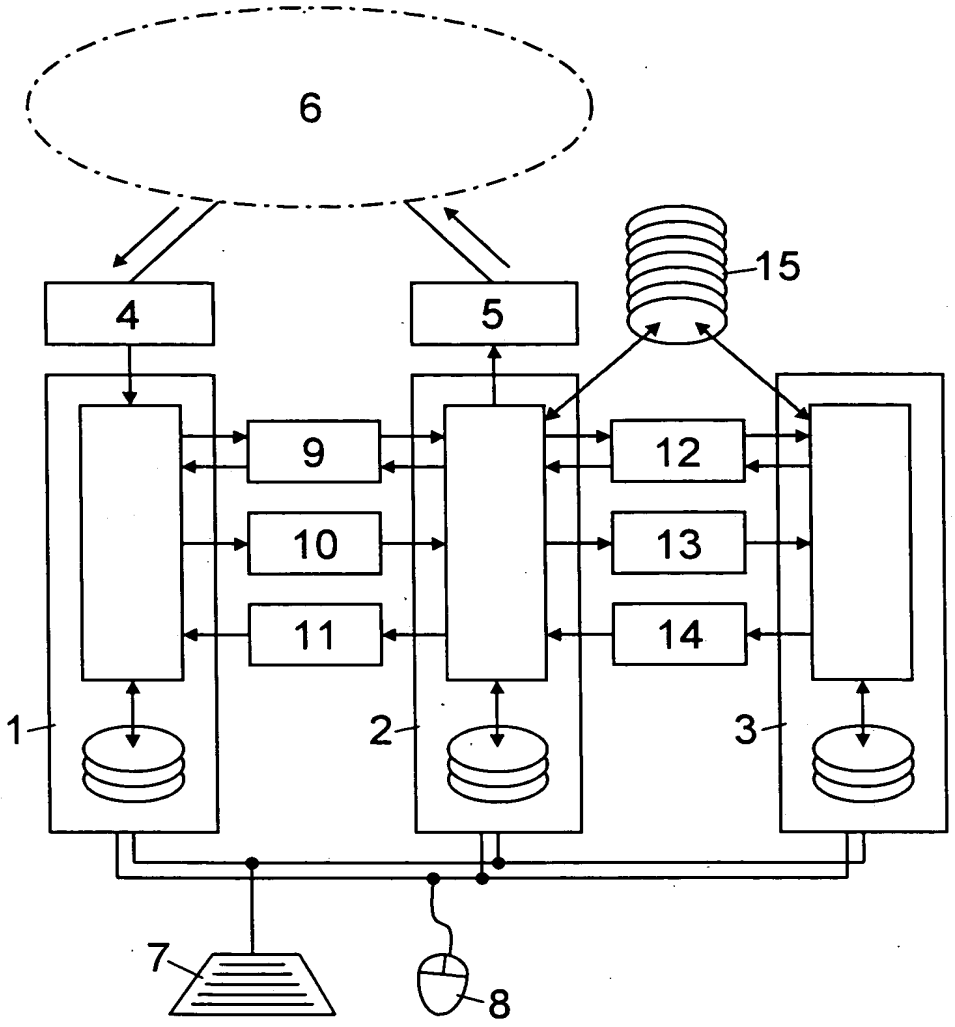
danter, dritter Rechner (3) vorgesehen ist und dass sich der zweite und der dritte Rechner (2, 3) durch Vergleich ihrer Arbeitsergebnisse abgleichen.

Zusammenfassung

Rechneranordnung, die an ein Datenübertragungsnetz anschließbar ist

Um bei einer Rechneranordnung, die an ein Datenübertragungsnetz anschließbar ist, einen sicheren Schutz gegen Computerviren, unerlaubte Zugriffe auf interne Daten und Datenverlust im Falle einer Infizierung zu erreichen, weist die Rechneranordnung einen ersten Rechner (1) und einen davon unabhängigen redundanten, zweiten Rechner (2) auf, wobei sich beide Rechner (1, 2) durch Vergleich ihrer Arbeitsergebnisse abgleichen, wobei der Empfang von Daten aus dem Datenübertragungsnetz (6) auf den ersten Rechner (1) und das Senden von Daten auf das Datenübertragungsnetz (6) auf den zweiten Rechner (2) beschränkt ist, wobei zumindest die Erst-Verarbeitung von empfangenen Daten auf den ersten Rechner (1) beschränkt ist und wobei von dem ersten Rechner (1) empfangene, nicht überprüfte oder nicht überprüfbare Daten nur verschlossen, d. h. nicht verarbeitbar, auf dem zweiten Rechner (2) gespeichert werden.

Figur


6
15
4
5
9
10
11
12
13
14
1
2
3
7
8